Registration Procedures and Forms for VIIS for Health Departments

STEP 1: DESIGNATE AN ADMINISTRATOR

o   The assigned administrator will be the main contact with the central office and will oversee the use of VIIS in their own organization. The central office is responsible for activating the administrator into the system. In turn, the administrator will use a simple procedure to activate all of their organization's users.

STEP 2: ASSIGNED ADMINISTRATOR MUST FILL OUT THE FOLLOWING THREE FORMS

o   VIIS User Registration Form
o   VIIS User Confidentiality Agreement
o   VDH Information Systems Security Access Agreement

STEP 3: MAIL OR FAX THE THREE FORMS COMPLETED BY THE ADMINISTRATOR TO THE FOLLOWING LOCATION*:

Mail the forms to   **Fax to:**
VIIS Support Staff   Fax to: (804) 864-8089
Virginia Department of Health   OR
Division of Immunization
109 Governor St. Rm 314 W
Richmond, VA 23219

* **IMPORTANT NOTE:** Only the completed forms in Step 2 are to be sent to VDH.

STEP 4: IN ADDITION, ADMINISTRATOR MUST HAVE EACH USER FILL OUT THE FOLLOWING THREE FORMS*:

o   VIIS User Registration Form
o   VIIS Security Policy & User Confidentiality Agreement

*IMPORTANT NOTE: These forms are to be maintained by the assigned administrator for the organization/site, they are NOT required to be mail to VDH.

STEP 5: YEARLY UPDATE

• Be sure to update your information yearly by filling out the "VIIS User Contact Information Update" form located under "Forms" at https://www.viis.virginia.gov

Virginia Immunization Information System (VIIS) User Registration Form

Must be accompanied by Organization/Site Registration form, if organization/site is not yet on VIIS.

1. Assigned Administrator:

_____
Printed Name, Title   Signature   Date

2. License number: _____

3. Phone: (_____)_____
4. Fax: (_____)_____

5. Alternate Phone: (_____)_____
6. Email: (_____)_____

7. Organization/Site Name: _____
8. VIIS Organization Code/Site Code _____ (If Known)

9. Address: _____
_____

10. VIIS Organization/Site Liaison:

_____
 Printed Name, Title   Signature   Date

 (_____)_____

13. Alternate Phone: (_____)_____
14. Email: (_____)_____

15. Last Name	16. First Name	17. Middle Name/ Initial	18. Professional Title	19. Position	20. VIIS Role*

VIIS Role Types: **RO**=*Reports Only* (View VIIS/Run Reports, NO Data Entry), **T**=*Typical User* (Enters Patient and Immunization Data, Runs Reports, NO Inventory Control), **IC**=*Inventory Control* (Enters Inventory, Patient, and Immunization Data, Runs Reports), **DE**=*Data Exchange* (Submits/Receives Files via VIIS Data Exchange Process/HMO) or **A**=*Administrator* (VIIS Organization/Site Administrator, sets up user accounts, views all modules)
TUR=*Typical User and Reports* – Allows Typical User to run ALL reports and not just Client-Specific Reports

VIIS Security Policy & User Confidentiality Agreement

VIIS Information:

The Code of Virginia, § 32.1-46.01 authorizes the Virginia Immunization Information System (VIIS), a statewide immunization information system that manages electronic immunization records. This policy states behaviors required of VIIS users, Virginia Department of Health (VDH), and Division of Immunization (DOI) to protect the confidentiality, privacy and accuracy of client information.

1. VIIS is consistent with the Department of Health and Human Services and the Health Insurance Portability and Accountability Act (HIPAA) of 1996.
2. Authorized users of VIIS will include:
   a. Health care provider or health plans
   b. Schools or other organizations that provide health care services
   c. Individuals or organizations as required by law or in the management of a public health crisis
   d. Other immunization registries
3. The review of this policy must involve the participation of representatives from the private and public health care sectors.

VDH/DOI Host Site Security:

1. The system will force users to change their password every 30 days.
2. The VIIS system will time-out after 45 minutes.
3. No information from VIIS will be made available to law enforcement, the Immigration and Naturalization Service, or any other party.
4. The VIIS system will maintain an audit trail for all information accessed.
5. VDH/ EDS will conduct a self-assessment of the potential risks and areas of vulnerability regarding VIIS and will develop, implement, and maintain appropriate security measures on an ongoing basis.
6. The release of immunization information shall be for statistical purposes or for studies that do not identify individuals.

Provider/ User Security:

1. Access to VIIS information is authorized under the condition that it is required to perform my job function
2. All VIIS users will be required to sign a Confidentiality/ Security Agreement with VDH
3. Each user must renew the user confidentiality/security agreement every two years.
4. Each user is responsible for maintaining confidentiality.
5. The provider will specify that the user has the obligation to act on any request by an individual to opt out of VIIS. If the patient elects to opt out, the provider should promptly mark the record in VIIS as "Do Not Share", so that only that provider may view the client's immunization records
6. The user will make reasonable effort to ensure the accuracy of all immunization and demographic information entered or edited
7. Virus protection is recommended for each client site.
8. User desktops/laptops must have physical security and password screen savers when not being used by authorized individuals and will terminate the VIIS application prior to leaving the VIIS workstation
9. An ID and Password are required to access VIIS.
10. Users will not share or disclose their ID or password to anyone.
11. The VIIS Administrator will maintain completed user registration forms in a secure location
12. All data from VIIS will be encrypted before transfer.
13. VIIS records will be treated with the same vigilance, confidentiality, and privacy as any other patient medical record.

14. Patient immunization records will not be copied except for authorized use
15. VIIS information in a paper copy will not be left where it would be visible for unauthorized personnel and must be shredded before disposal
16. Unauthorized disclosure of information from confidential records may be punishable, upon conviction, by a fine and/or imprisonment or both, and/or civil penalties as prescribed by law as well as sanctions and/or disciplinary action.
17. If VIIS data is to be faxed, the sender must verify the fax number and receipt of data.
18. Any activity that would jeopardize the proper function/security of VIIS will not be conducted. Misuse of VIIS may result in legal action against me personally, and against the organization for which I am an agent

Provider Responsibility:

1. A copy of this agreement has been provided to me
2. The VIIS Administrator at the user site will terminate access for an authorized user who no longer requires access.
3. Users will make every effort to protect VIIS screens from unauthorized view.
4. Should a material breach of personal privacy/confidentiality occur, the offending party must immediately notify the client and VDH/ DOI designee. Violators of this policy will be restricted from VIIS by the System Administrator at the offender's site.
5. The VIIS Administrator will be notified immediately if unauthorized entry into the system is suspected.

Approved by:

To be signed by one representative that has the delegated authority to act on behalf of the User organization and one representative that has the delegated authority to act on behalf of VDH/DOI.

_____
User Company/Organization Name (Print)

_____   _____
Name of Authorized Agent (Print)   Name of Authorized Agent (Print)

_____   _____
Signature of Authorized Agent   Signature of Authorized Agent

_____   _____
Title   Title

_____   _____
Date   Date

Reviewed on 11-02-2007